LGPD

Lei Geral de Proteção de Dados

Fernando Silveira

Qual o objetivo da nova Lei de Proteção de Dados Pessoais (“LGPD”)?

A Lei nº 13.709, de 14 de agosto de 2018, também conhecida como Lei Geral de Proteção de Dados (“LGPD”) do Brasil.

Aplicação: Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Novos conceitos de dados

- **Dados simples:** informações genéricas, que podem corresponder aos números de visitantes do seu site, por exemplo.
- **Dados pessoais:** informações que identifiquem o usuário assim que o dado simples recebe o primeiro tratamento, como o nome.
- **Dados sensíveis:** informações sobre gênero, raça/etnia, religião, ideologia política ou filosófica, entre outros dados.
- **Dados anonimizados:** informações de um usuário que não pode ser identificado.

Outras leis semelhantes

- General Data Protection Regulation (GDPR) - 25 de maio de 2018
- California Consumer Privacy Act - 28 de junho de 2018

Figuras

O CONTROLADOR: Empresas que detém os dados, isto é, que armazenam informações.
O OPERADOR: é a empresa que realiza o tratamento e processamento de dados pessoais sob as ordens do controlador.

O TITULAR: é a pessoa física a quem se referem os dados pessoais.

Encarregado de Proteção de Dados (DPO)

Trata-se de um trabalhador da empresa ou um consultor externo que assume a responsabilidade formal, pela conformidade com a legislação de proteção de dados dentro da empresa.

- Conhecimento em riscos, compliance, tecnologia e segurança.
- Monitorização regular e sistemática de dados pessoais em grande escala;
- Cargo com nível de C-Level
- Pessoa que vai comunicar a autoridade.

A nomeação de um Encarregado de Proteção de Dados **só será obrigatória** quando e entidade em causa reunir uma das seguintes condições : **Ser um organismo público**, **tratar dados pessoais em grande escala e de forma sistemática** (ex: Bancos) ou **tratar categorias especiais de dados pessoais em grande escala**.

Princípios da LGPD

- **Finalidade:** legítimas, específicas, explícitas e conhecidas do titular;
- **Adequação:** compatível com a finalidade e com as expectativas do titular, não excessivos;
- **Necessidade:** mínimo necessário para as finalidades almejadas;
- **Livre acesso:** modalidades de tratamento e a integridade de seus dados pessoais;
- **Qualidade dos dados:** exatidão, clareza, necessidade e atualização dos dados durante todo o seu ciclo de vida;
- **Transparência:** informações claras e adequadas sobre o tratamento;
- **Segurança:** medidas de proteção proporcionais para a proteção contra acessos não autorizados;
- **Prevenção:** prevenir a ocorrência de danos em virtude do tratamento;
- **Discriminação:** tratamento não pode ser realizado para fins discriminatórios, que mitiguem direitos dos titulares Princípios (aplicabilidade geral)
- **Responsabilidade e Prestação de contas:** Demonstração de adoção de medidas eficazes ao cumprimento das normas.

http://bit.ly/2OXFbrg

Quem pode coletar dados?

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

1. Consentimento
2. **Cumprimento de obrigação Legal**
3. Execução de políticas públicas
4. Estudos por Órgão de Pesquisa
5. **Execução de Contrato/Diligências Pré contratuais**
6. Exercício Regular de Direitos
7. Proteção da Vida
8. Tutela da Saúde
9. **Interesse Legítimos do Controlador/Terceiro**
10. Proteção ao Crédito

http://bit.ly/2yJaR9V

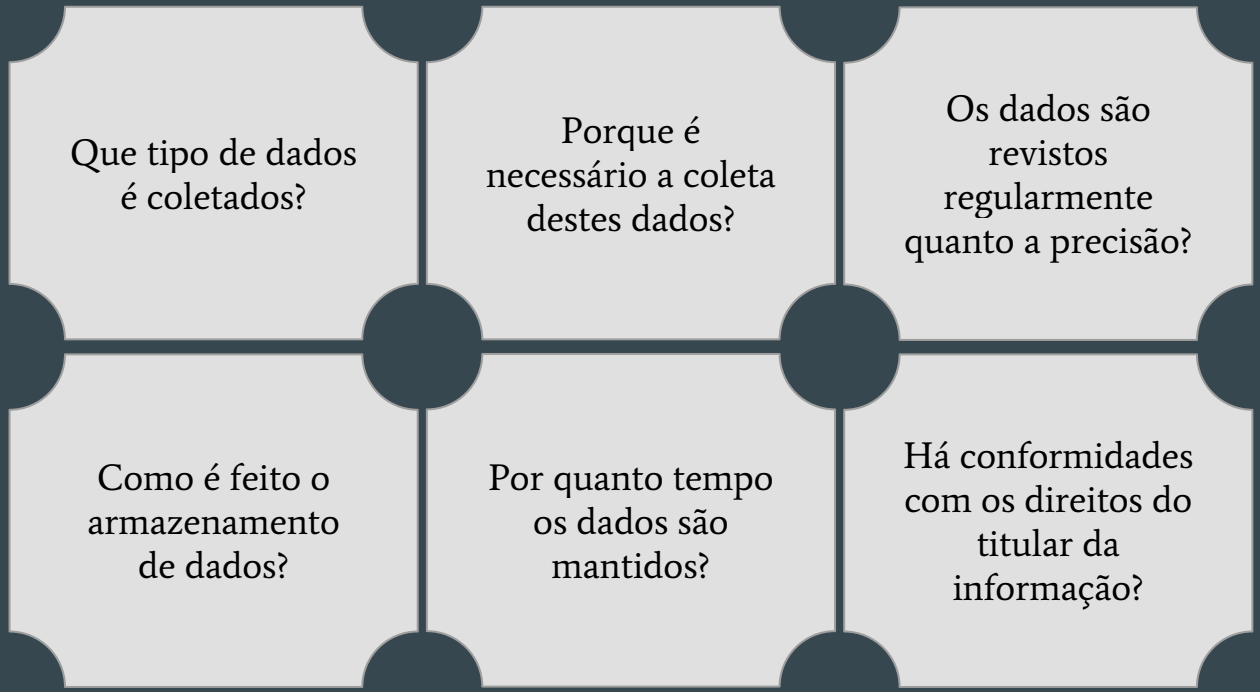
Eu colhi o consentimento, então posso fazer o que quiser com os dados?

Não! O tratamento que será dado aos dados precisa estar de acordo com os princípios da LGPD, entre os quais está o da **finalidade** e **adequação**.

Conheça seus dados

A LGPD vale para as empresas que coletam dados pessoais, ou seja, informações que podem identificar alguém, seja no universo online, como no offline. Além de dados como nome, RG e CPF, a lei prevê também o tratamento de dados sensíveis, como informações de origem racial ou étnica, de saúde, religião e opinião política.

Desafio de Governança



http://bit.ly/2AFFZbz

Proteja seus dados

Garantir que os controles certos de segurança estejam em ordem para proteger as informações.

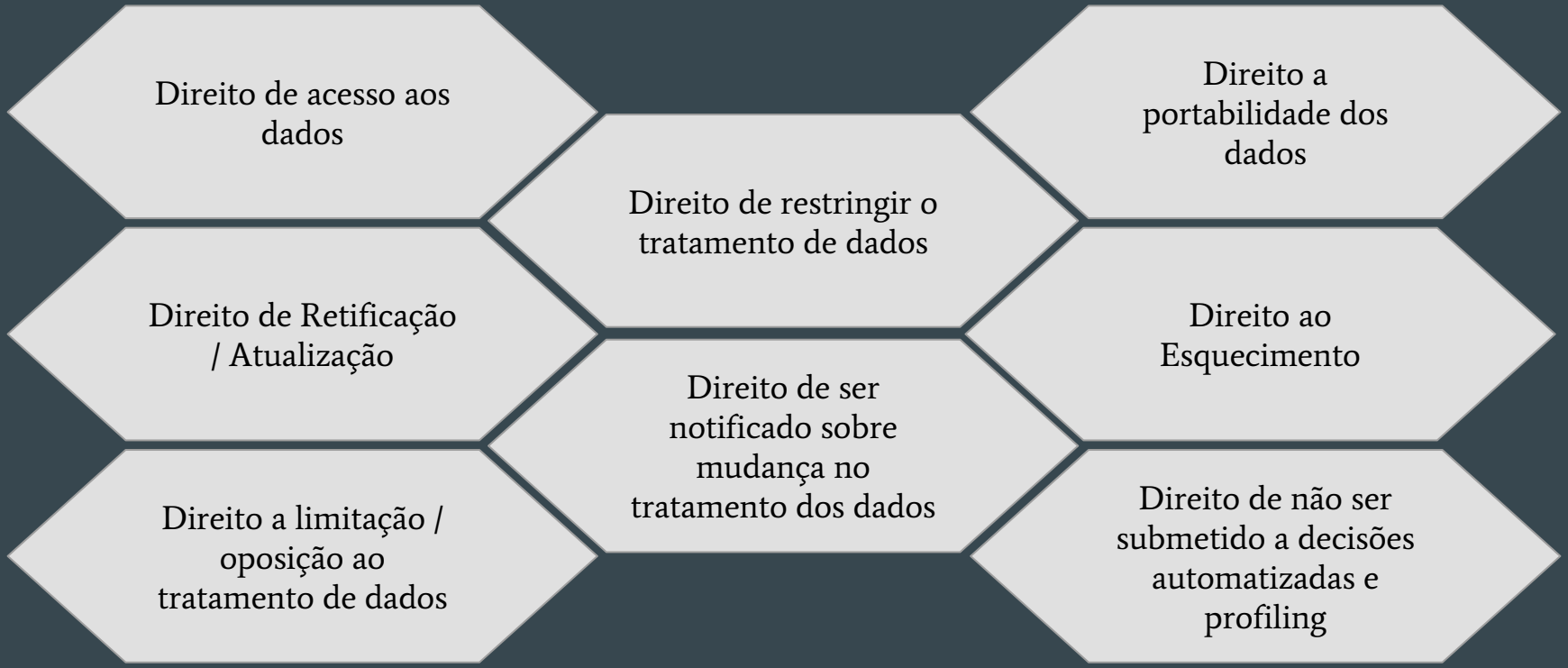
- Criptografia
- Fluxos de trabalho padronizados
- Educação interna
- Controle de acesso
- Soluções de backup

Minimização dos dados

Abordagem de “Minimização dos dados”, onde não captem informações a menos que sejam necessárias.

As informações de identificação pessoal são mais do que apenas o seu nome, morada, e-mail e número de telefone. Também inclui endereços IP, identificação do dispositivo e geolocalização, porque se reunir o suficiente desses pontos de dados pode identificar a pessoa.

Direitos do titular da informação



http://portaldaprivacidade.com.br/2018/09/10/infografico-08-direitos-dos-titulares-na-lgpd/

Quando a LGPD entrará em vigor?

A LGPD entrará em vigor após 18 meses da sua publicação. Uma vez que a LGPD foi publicada em 15 de agosto de 2018 sua entrada em vigor acontecerá em fevereiro de 2020.

Haverá um órgão responsável pela aplicação e fiscalização da LGPD?

Existem alguns dispositivos da LGPD que preveem uma autoridade nacional responsável por zelar, implementar e fiscalizar o cumprimento da LGPD. Apesar de previsto e mencionado na LGPD, esse órgão ainda não foi criado. Sua criação depende de iniciativas e participação do Governo e do Congresso

Comunicados

Caso violada a segurança dos dados pessoais de modo a acarretar risco ou dano relevante aos seus titulares, a LGPD dispõe que o Controlador deverá comunicar à Autoridade Nacional e ao titular, indicando, dentre outras informações, a natureza dos dados afetados, os riscos relacionados ao incidente e as medidas adotadas para reverter ou mitigar prejuízos.

- Comunicação em um prazo razoável.

Penalidades

Art. 52 - Elas englobam advertência, multa ou até mesmo a proibição total ou parcial de atividades relacionadas ao tratamento de dados. As multas podem variar de 2% do faturamento do ano anterior até a R$ 50 milhões, passando por penalidades diárias.

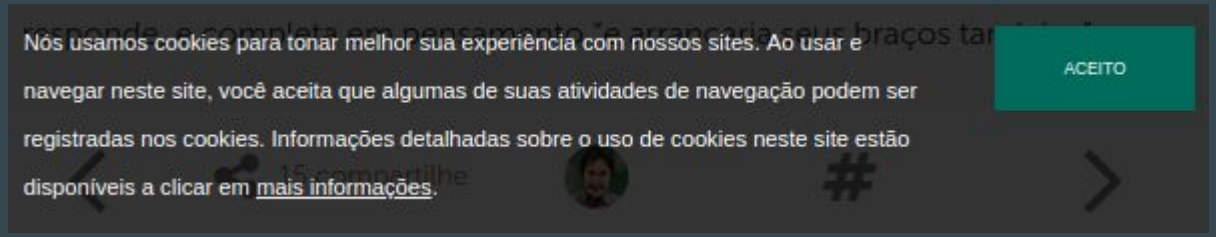
Exposição na Mídia e perda de confiança dos clientes.

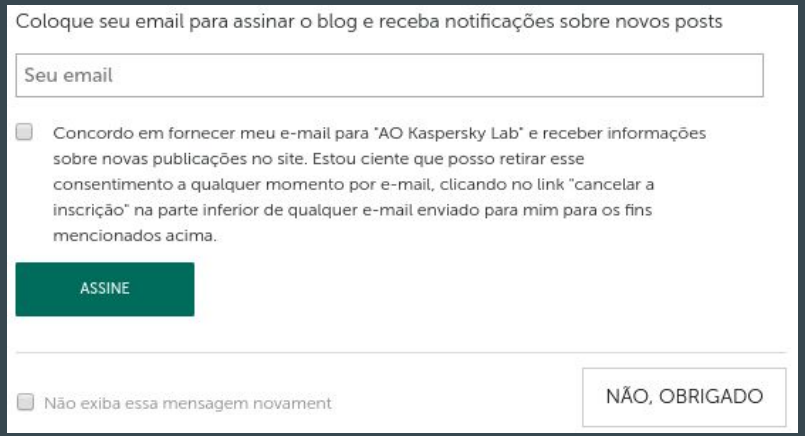
E a GDPR ?

- Começou a vigorar a partir de 25 de maio
- Evolução da Diretiva Européia de 1995 (Diretiva 95/46/CE)
- Cultura de quase 25 anos
- Independentemente da localização das empresas
- Os dados não podem ser trazidos para o brasil.
- Multa de 4% sobre o volume de negócios anual ou de 20 milhões de euro
- 72 horas para que o vazamento de dados seja informado à comissão de proteção de dados.

http://www.pinheironeto.com.br/Pages/publicacoes-detalhes.aspx?nID=1362

Formulários WEB





O que temos de cadastro para e-mail marketing é necessário entrar em contato com o cliente para obter o consentimento. Devemos guardar este consentimento.

Temos 14 meses!

- Política de privacidade do site;
- Políticas de privacidade internas (por exemplo, política de privacidade do funcionário, política do escudo de privacidade do código de conduta – se aplicável);
- Padrões de classificação de dados;
- Padrões de solicitação de acesso a dados;
- Política de mídia social.

- Diretrizes de gerenciamento de fornecedores, padrões de fornecedores e due diligence;
- Política de uso aceitável (também BYOD, Monitoramento, etc.);
- Violação de dados, política de resposta a incidentes e procedimentos;
- Treinamento de funcionários;
- Classificação e gerenciamento de dados.

- Normas e requisitos de segurança;
- Política de Utilização Aceitável;
- Software de prevenção de perda de dados;
- Inventário de dispositivos;
- Controle de mídia removível; e,
- Controle de acesso, provisionamento, logs e outras relacionadas às questões técnicas de proteção da informação.

- Políticas de retenção de dados;
- Política de desligamento de funcionários;
- Política de backups;
- Política de continuidade de negócios e contingência.

Obrigado!

...

Fernando Silveira
fernandosilveira@outlook.com